

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 2

PATENT
Filed: January 26, 2001

1. (currently amended) A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ; [and]
encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K ;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein each subset S_{i1}, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key, wherein content is provided to users in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of users in the revoked set R and N is the total number of users.

2. (canceled).
3. (currently amended) The method of Claim [2]1, wherein the tree is a complete binary tree.
4. (original) The method of Claim 1, further comprising using private information I_u to decrypt the session key.

1053-121, AM2

CASE NO.: ARC9-2001-0005-US1
 Serial No.: 09/770,877
 April 26, 2005
 Page 3

PATENT
 Filed: January 26, 2001

5. (original) The method of Claim 4, wherein the act of decrypting includes using information i_j such that a user belongs to a subset S_{ij} , and retrieving a subset key L_{ij} using the private information of the user.

6. (canceled).

7. (canceled).

8. (currently amended) The method of Claim [6]1, wherein each user must store $\log N$ keys, wherein N is the total number of users.

9. (currently amended) ~~The method of Claim 6~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information L_i ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_{11}, \dots, S_{1m} having associated subset keys L_{11}, \dots, L_{1m} ; [and]
encrypting the session key K with the subset keys L_{11}, \dots, L_{1m} to render m encrypted versions of the session key K ;
partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree, wherein each subset S_{11}, \dots, S_{1m} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key, wherein

1033-121.AM2

CASE NO.: ARC9-2001-0005-US1
 Serial No.: 09/770,877
 April 26, 2005
 Page 4

PATENT
 Filed: January 26, 2001

content is provided to users in at least one message, and wherein each user processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of users.

10. (currently amended) The method of Claim [6]1, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

11. (currently amended) The method of Claim [2]1, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

12. (currently amended) ~~The method of Claim 11~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information L_i ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_{s_1}, \dots, L_{s_m} ;
encrypting the session key K with the subset keys L_{s_1}, \dots, L_{s_m} to render m encrypted versions of the session key K ;
partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 5

PATENT

Filed: January 26, 2001

node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein content is provided to users in at least one message defining a header, and the header includes at most $2r-1$ subset keys and encryptions, wherein r is the number of users in the revoked set R .

13. (currently amended) ~~The method of Claim 11~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information L_i ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_{s1}, \dots, L_{sm} ;

encrypting the session key K with the subset keys L_{s1}, \dots, L_{sm} to render m encrypted versions of the session key K ;

partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein each user must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of users.

14. (currently amended) ~~The method of Claim 11~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information L_i ;
selecting at least one session encryption key K ;

1003-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 6

PATENT
Filed: January 26, 2001

partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_1, \dots, L_m ;

encrypting the session key K with the subset keys L_1, \dots, L_m to render m encrypted versions of the session key K;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein content is provided to users in at least one message, and wherein each user processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of users.

15. ~~The method of Claim 14~~ A method for broadcast encryption, comprising:

assigning each user in a group of users respective private information I_i ;

selecting at least one session encryption key K;

partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_1, \dots, L_m ;

encrypting the session key K with the subset keys L_1, \dots, L_m to render m encrypted versions of the session key K;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 7

PATENT

Filed: January 26, 2001

node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein the revoked set R defines a spanning tree, and wherein the method includes:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

16. ~~The method of Claim 11~~ A method for broadcast encryption, comprising:

assigning each user in a group of users respective private information L_i ;

selecting at least one session encryption key K ;

partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_{11}, \dots, L_{1m} ;

encrypting the session key K with the subset keys L_{11}, \dots, L_{1m} to render m encrypted versions of the session key K ;

partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein each node has at least one label possibly induced by at least one of its ancestors, and wherein each user is assigned labels from all nodes hanging from a direct path between the user and the root but not from nodes in the direct path.

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 8

PATENT
Filed: January 26, 2001

17. (original) The method of Claim 16, wherein labels are assigned to subsets using a pseudorandom sequence generator, and the act of decrypting includes evaluating the pseudorandom sequence generator.

18. (currently amended) ~~The method of Claim 1~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information L_i ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated
subset keys L_{s1}, \dots, L_{sm} ; and
encrypting the session key K with the subset keys L_{s1}, \dots, L_{sm} to render m encrypted versions
of the session key K , wherein content is provided to users in at least one message having a header including a cryptographic function E_r , and the method includes prefix-truncating the cryptographic function E_r .

19. (currently amended) The method of Claim [2]1, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each user is assigned keys from all nodes in a direct path between a leaf representing the user and the root.

20. (currently amended) ~~The method of Claim 1~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information L_i ;
selecting at least one session encryption key K ;

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 9

PATENT
Filed: January 26, 2001

partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ; and
encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K, wherein content is provided to users in at least one message defining plural portions, and each portion is encrypted with a respective session key.

21. (currently amended) A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key; [and]

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers, wherein logic means provide content to receivers in at least one message, and wherein each receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

22. (original) The computer program device of Claim 21, further comprising:

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} .

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 10

PATENT
Filed: January 26, 2001

23. (original) The computer program device of Claim 22, further comprising logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree.

24. (original) The computer program device of Claim 21, further comprising logic means for using private information I_u to decrypt the session key.

25. (original) The computer program device of Claim 24, wherein the means for decrypting includes logic means for using information i_j such that a receiver belongs to a subset S_{ij} , and retrieving a key L_{ij} from the private information of the receiver.

26. (original) The computer program device of Claim 23, wherein each subset S_{ij}, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key.

27. (currently amended) ~~The computer program device of Claim 26~~ A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

1003-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 11

PATENT

Filed: January 26, 2001

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers, wherein logic means provide content to receivers in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R and N is the total number of receivers.

28. (original) The computer program device of Claim 26, wherein each receiver must store $\log N$ keys, wherein N is the total number of receivers.

29 (canceled).

30. (original) The computer program device of Claim 26, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

31. (original) The computer program device of Claim 23, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 12

PATENT

Filed: January 26, 2001

32. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message
to plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_1, \dots, S_m
having associated subset keys L_1, \dots, L_m ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and
the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node
having at least one associated label, and wherein each subset includes all leaves in a subtree rooted
at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i ,
wherein logic means provide content to receivers in at least one message defining a header, and the
header includes at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the
revoked set R.

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 13

PATENT
Filed: January 26, 2001

33. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message
to plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_1, \dots, S_m
having associated subset keys L_1, \dots, L_m ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and
the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node
having at least one associated label, and wherein each subset includes all leaves in a subtree rooted
at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i ,
wherein each receiver must store $.5 \log^2 N + .5 \log N + 1$ keys, wherein N is the total number of
receivers.

34. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 14

PATENT
Filed: January 26, 2001

a computer program storage device including a program of instructions usable by a computer,
comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message
to plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_1, \dots, S_m
having associated subset keys L_1, \dots, L_m ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and
the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node
having at least one associated label, and wherein each subset includes all leaves in a subtree rooted
at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i ,
wherein logic means provide content to receivers in at least one message, and wherein each receiver
processes the message using at most $\log N$ operations plus a single decryption operation, wherein N
is the total number of receivers.

35. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 15

PATENT
Filed: January 26, 2001

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_1, \dots, L_m ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein the revoked set R defines a spanning tree, and wherein ~~(original)~~ The the computer program device includes:

logic means for initializing a cover tree T as the spanning tree; and

logic means for iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

1003-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 16

PATENT
Filed: January 26, 2001

36. (original) The computer program device of Claim 35, wherein logic means assign labels to receivers using a pseudorandom sequence generator, and the labels induce subset keys.

37. (original) The computer program device of Claim 36, wherein the means for decrypting includes evaluating the pseudorandom sequence generator.

38. (currently amended) ~~The computer program device of Claim 21~~ A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key; and

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers, wherein logic means provide content to receivers in at least one message having a header including a cryptographic function E_L , and (original) The the computer program device includes logic means for prefix-truncating the cryptographic function E_L .

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 17

PATENT

Filed: January 26, 2001

39. (original) The computer program device of Claim 23, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein logic means assign each receiver keys from all nodes in a direct path between a leaf representing the receiver and the root.

40. (currently amended) ~~The computer program device of Claim 21~~ A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key; and

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers, wherein logic means provide content to receivers in at least one message defining plural portions, and each portion is encrypted with a respective session key.

41. (currently amended) A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content; [and]

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 18

PATENT

Filed: January 26, 2001

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein each subset S_{j1}, \dots, S_{jm} includes all leaves in a subtree rooted at some node v_j , at least each node in the subtree being associated with a respective subset key, wherein content is provided to receivers in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R and N is the total number of receivers.

42. (original) The computer of Claim 41, wherein the method acts further comprise:

assigning each receiver in a group of receivers respective private information I_v ;

selecting at least one session encryption key K ;

partitioning all receivers not in a revoked set R into disjoint subsets S_{j1}, \dots, S_{jm} having associated subset keys L_{j1}, \dots, L_{jm} ; and

encrypting the session key K with the subset keys L_{j1}, \dots, L_{jm} to render m encrypted versions of the session key K .

43. (canceled).

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 19

PATENT
Filed: January 26, 2001

44. (currently amended) The computer of Claim [43]~~41~~, wherein the tree is a complete binary tree,

44. (canceled).

45. (original) The computer of Claim 44, wherein the act of decrypting undertaken by the computer includes using information i , such that a receiver belongs to a subset S_i , and retrieving a key L_i using the private information of the receiver.

46. (canceled).

47. (canceled).

48. (currently amended) The computer of Claim [46]~~41~~, wherein each receiver must store $\log N$ keys, wherein N is the total number of receivers.

49. (currently amended) The computer of Claim 46 A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content; and

sending the broadcast content to plural stateless receivers and to at least one revoked receiver

such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 20

PATENT
Filed: January 26, 2001

content, wherein content is provided to receivers in at least one message, and wherein each receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

50. (currently amended) The computer of Claim [46]41, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

51. (original) The computer of Claim 41[43], wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

52. (original) The computer of Claim 51, wherein content is provided to receivers in at least one message defining a header, and the header includes at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R .

53. (original) The computer of Claim 51, wherein each receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

54. (original) The computer of Claim 51, wherein content is provided to receivers in at least one message, and wherein each receiver processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 21

PATENT
Filed: January 26, 2001

55. (original) The computer of Claim 51, wherein the revoked set R defines a spanning tree, and wherein the method acts undertaken by the computer further include:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

56. (original) The computer of Claim 55, wherein the computer assigns node labels to receivers from the tree using a pseudorandom sequence generator.

57. (original) The computer of Claim 56, wherein the act of decrypting undertaken by the computer includes evaluating the pseudorandom sequence generator.

58. (currently amended) ~~The computer of Claim 44~~ A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content;

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content, wherein content is provided to receivers in at least one message having a header including a cryptographic function E_i , and the method acts undertaken by the computer include prefix-truncating the cryptographic function E_i .

1053-121.AM7

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 22

PATENT
Filed: January 26, 2001

59. (currently amended) ~~The computer of Claim 41~~ A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content;

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content, wherein content is provided to receivers in at least one message defining plural portions, and each portion is encrypted by the computer with a respective session key.

60. (original) The method of Claim 11, wherein each node has plural labels with each ancestor of the node inducing a respective label, and wherein each user is assigned labels from all nodes hanging from a direct path between the user and the root but not from nodes in the direct path.

61-64. (canceled).

65. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in at least one

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 23

PATENT
Filed: January 26, 2001

message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of receivers in a revoked set R and N is the total number of receivers.

66. (original) The receiver of Claim 65, wherein the receiver is partitioned into one of a set of groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree defining nodes and leaves.

67. (original) The receiver of Claim 66, wherein subsets S_{i1}, \dots, S_{im} derived from the set of groups S_1, \dots, S_w define a cover.

68. (canceled).

69. (original) The receiver of Claim 67, wherein the receiver must store $\log N$ keys, wherein N is the total number of receivers.

70. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in at least one

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 24

PATENT

Filed: January 26, 2001

message defining a header, and wherein the receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

71. (original) The receiver of Claim 67, wherein a revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

72. (original) The receiver of Claim 67, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

73. (previously presented) A receiver of content, comprising:

- means for storing respective private information I_u ;
- means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and
- means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in a message having a header including at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R .

74. (previously presented) A receiver of content, comprising:

- means for storing respective private information I_u ;

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 25

PATENT
Filed: January 26, 2001

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

75. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein content is provided to the receiver in at least one message, and wherein the receiver processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

76. (original) The receiver of Claim 72, wherein the receiver decrypts the subset key by evaluating a pseudorandom sequence generator.

77. (previously presented) A receiver of content, comprising:

a data storage storing respective private information I_u ;

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1

Serial No.: 09/770,877

April 26, 2005

Page 26

PATENT

Filed: January 26, 2001

a processing device receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content, the processing device obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in at least one message defining a header, and wherein the receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

78. (original) The receiver of Claim 77, wherein the receiver is partitioned into one of a set of groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree.

79. (original) The receiver of Claim 78, wherein subsets S_{i1}, \dots, S_{im} derived from the set of groups S_1, \dots, S_w define a cover.

80. (original) The receiver of Claim 79, wherein the receiver receives content in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of receivers in a revoked set R and N is the total number of receivers.

81. (original) The receiver of Claim 79, wherein the receiver must store $\log N$ keys, wherein N is the total number of receivers.

82. (canceled).

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1
Serial No.: 09/770,877
April 26, 2005
Page 27

PATENT
Filed: January 26, 2001

83. (original) The receiver of Claim 79, wherein one revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

84. (original) The receiver of Claim 79, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

85. (original) The receiver of Claim 84, wherein the receiver receives content in a message having a header including at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R .

86. (original) The receiver of Claim 84, wherein the receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

87. (original) The receiver of Claim 84, wherein content is provided to the receiver in at least one message, and wherein the receiver processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

88. (original) The receiver of Claim 84, wherein the receiver decrypts the subset key by evaluating a pseudorandom sequence generator.

1053-121.AM2

CASE NO.: ARC9-2001-0005-US1**Serial No.: 09/770,877****April 26, 2005****Page 28****PATENT****Filed: January 26, 2001**

89-94 (canceled).

95. (currently amended) The computer of Claim [42]41, wherein the act of partitioning is undertaken by a system computer in a system of receivers separate from the system computer.

96. (currently amended) The computer of Claim [42]41, wherein the act of partitioning is undertaken by a receiver computer.

97. (original) The receiver of Claim 67, wherein the receiver derives the subsets in the cover.

98. (previously presented) The computer of Claim 41, wherein the method acts include using private information I_s to decrypt the session key.

1053-121.AM2